§ 3. Прости числа. Основна теорема на аритметиката

**Определение.** Едно естествено число  се нарича *просто*, ако единствените му делители са  и . Еквивалентно: *p* не може да се представи като произведение на две естествени числа, по-малки от него. Едно число  се нарича *съставно*, ако не е просто. (Числото 1 играе особена роля и не е нито просто, нито съставно.)

**Твърдение 3.1.** *Всяко естествено число  притежава поне един прост делител. При това, ако n е съставно число, то n притежава прост делител .*

*Доказателство.* Нека *p* е най-малкият положителен делител на *n*, по-голям от 1. Тогава *p* е просто число. Действително, в противен случай числото *p* би имало делител, по-голям от 1 и по-малък от *p*, който е делител и на *n*, противоречие с избора на *p*. Освен това, ако *n* е съставно число, то  и (отново от избора на *p*) . Оттук следва  (ако , то и  и , противоречие).

**Теорема 3.2 (Евклид).** *Съществуват безбройно много прости числа.*

*Доказателство.* Да допуснем противното и нека  са всички прости числа. Според твърдение 3.1 числото  притежава поне един прост делител *p* и значи  за някое . Но тогава , противоречие.

**Упражнение 3.3.** *Нека p е просто число. Да се докаже, че условието  е еквивалентно с условието .*

**Твърдение 3.4.** *Нека p е просто число. Ако  и , то  . По-общо, ако p дели произведението на няколко числа, то p дели поне едно от тях.*

*Доказателство.* Тъй като *p* е просто число, условието ** е еквивалентно с условието . Сега твърдението следва директно от твърдение 2.3. Така, ако *p* дели произведението на две числа, то *p* дели поне едното от тях (в действителност, това е необходимо и достатъчно условие *p* да бъде просто число). Обобщението за повече от две числа се доказва по индукция.

**Теорема 3.5 (Основна теорема на аритметиката).** *Всяко естествено число  се представя като произведение на прости числа и това представяне е единствено с точност до реда на простите множители.*

*Доказателство.* **1) Съществуване на представянето.** Ще проведем индукция по *n*. При  това е очевидно. Нека  и да допуснем, че твърдението е доказано за всички естествени числа, по-големи от 1 и по-малки от *n*. Ако *n* е просто число, имаме очевидното представяне  . Ако *n* е съставно число, то , където  и  са естествени числа, по-малки от *n* (и по-големи от 1). Според индукционното предположение всяко от числата  и  е произведение на прости числа, откъдето получаваме търсеното представяне и за *n*.

**2) Единственост.** Нека , където  и  са прости числа. Простото число  дели *n* и значи дели произведението . Според твърдение 3.4  дели някой от множителите в това произведение, например . Но  също е просто число, следователно . Тогава . Продължавайки по същия начин, се уверяваме, че  и (след евентуално преномериране)  за всяко . Теоремата е доказана.

**Забележка 1.** В представянето на едно естествено число  като произведение на прости числа можем да обединим равните прости множители и да получим единствено представяна на *n* във вида

,

където  са различни прости числа и . Това представяне се нарича *канонично разлагане на n в произведение на прости множители.*

**Забележка 2.** Нека *a* и *b* са естествени числа и в каноничното разлагане на произведението *ab* участват простите множители  Тогава можем да запишем

,

където . Да означим

 .

Тогава **.

**Упражнение 3.6.** *Нека p е просто число. Да се докаже, че за всяко  биномният коефициент  се дели на p.*